

Efficient Patterns for Model Checking Partial State Spaces in $CTL \cap LTL$

Adam Antonik¹ & Michael Huth¹

¹Department of Computing
Imperial College London

Talk for MFPS 22, 26 May 2006
Genova, Italy

- 1 Introduction
- 2 Motivation & results
- 3 Summary & related work

Partial spate spaces (Bruns & Godefroid'99)

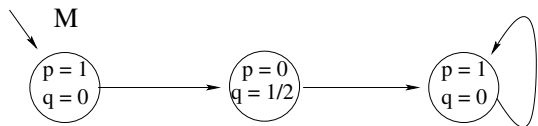
- state set & transition relation as for Kripke structures
- atomic observable p may be true (1), false (0) or unknown (1/2) at state s :

$$L(s, p) \in \{0, 1/2, 1\}$$

- new ingredient: $L(s, p) = 1/2$ expresses *partiality* of state, the truth value of p as s is unknown/not specified.
- well understood: partiality enables aggressive abstraction and sound checks of abstractions for properties that mix path quantifiers (e.g. “the system can always recover”).

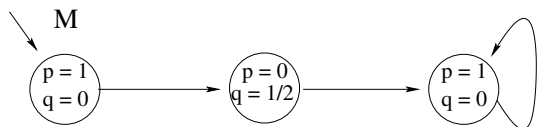
Example model (Bruns & Godefroid'00)

```
void someArithmetic() {  
    x,y = 1,0; // concurrent assignments  
    x,y = 2*f(x),f(y);  
    x,y = x+1,0; }  
}
```



- $f: \text{int} \rightarrow \text{int}$ **unknown function**
- **finite-state** model M above obtained by **predicate abstraction** from infinite-state program above: $p = \text{"x is odd"}$ and $q = \text{"y is odd"}$

Example model check (Bruns & Godefroid'00)



- $M \not\models EG\neg q \vee EF(\neg p \wedge q)$ note **mixed polarity** for q
- definition of \models as usual, except for literals:
 - $s \models p$ iff $L(s, p) = 1$
 - $s \models \neg p$ iff $L(s, p) = 0$
 - and so $s \not\models p \vee \neg p$ whenever $L(s, p) = 1/2$
- But: all Kripke structures that **implement** M (i.e. that resolve all 1/2 somehow into 1 or 0) satisfy $EG\neg q \vee EF(\neg p \wedge q)$

Thorough semantics and semantic minimization

- $M \models^{th} \phi$ iff all implementations of M satisfy ϕ
- soundness holds: $M \models \phi \Rightarrow M \models^{th} \phi$
- ϕ^p pessimistic semantic minimization of ϕ iff
(for all M , $M \models \phi^p \Leftrightarrow M \models^{th} \phi$)
- dual: ϕ^o optimistic semantic minimization of ϕ iff
 $\neg\phi^o$ is pessimistic semantic minimization of $\neg\phi$
- we speak of *self-minimization* whenever ϕ can be chosen as ϕ^p or ϕ^o
- Example: $EF(p \wedge AX(\neg p))$
“a p -state, whose next states aren't p -states, is reachable”
not pessimistically self-minimizing but has

$$EF(p \wedge AF(\neg p))$$

as pessimistic semantic minimization.

Existing results (Godefroid & H.'05)

- all CTL formulas have pessimistic semantic minimization in modal mu-calculus
- CTL formula $\neg A[(EXq_1)U(q_1 \rightarrow q_2)]$ has no pessimistic semantic minimization in CTL or CTL*
- computing pessimistic semantic minimization for CTL is EXPTIME-hard

Empirical question of this paper

- Most frequently used specification patterns in practice are in $CTL \cap LTL$ and documented at

`patterns.projects.cis.ksu.edu`

- Empirical question: Are pessimistic minimizations for all these patterns expressible in $CTL \cap LTL$, and with linear blowup only?
- This paper answers this question in the affirmative.

Method of proof for self-minimization

- patterns that are pessimistically self-minimizing are all classified as such through two mutually dependent grammars that generate only formulas that are pessimistically or optimistically self-minimizing
- these grammars are suitable extensions of those in (Godefroid & H.05)
- example of new grammar clause: if ϕ and ψ are pessimistically self-minimizing and ϕ is in propositional logic, then $\phi \wedge AX\psi$ is pessimistically self-minimizing

Method of proof for linear blowup of pattern

- patterns that are not pessimistically self-minimizing have only one atom in mixed polarity, e.g. $A[\neg P \vee AG(\neg R)WR]$
- for such patterns ϕ we construct pessimistic semantic minimization ϕ^P using our grammars, semantic equivalences, and the following

(Principle): ψ is pessimistic semantic minimization of ϕ if ψ is pessimistically self-minimizing and equivalent to ϕ over Kripke structures.
- for some patterns, we also use that valid formulas are optimistically self-minimizing, and unsatisfiable formulas are pessimistically self-minimizing.

Examples of pessimistically self-minimizing patterns

- Absence of P ; After Q until R :

$$AG(Q \wedge \neg R \rightarrow A[\neg PWR])$$

- Response chain: 2 stimuli, 1 response; After Q :

$$\neg E[\neg QU(Q \wedge EF(S \wedge EX(EF(T \wedge EG(\neg P))))))]$$

- Precedence chain: 2 stimuli, 1 response; after Q until R :

$$AG(Q \rightarrow \neg E[(\neg S \wedge \neg R)U(P \wedge \neg R)] \wedge \neg E[(\neg P \wedge \neg R)U(S \wedge \neg P \wedge \neg R \wedge EX(E[(\neg T \wedge \neg R)U(P \wedge \neg T \wedge R)]))])$$

Example of linear blowup of non-self-minimizing pattern

- consider pattern

$$A[\neg P \vee AG(\neg R)WR] \tag{1}$$

- by definition of AW, negation of (1) is

$$E[\neg RU(\neg R \wedge \neg(\neg P \vee AG(\neg R)))] \tag{2}$$

- suffices to compute optimistic semantic minimization for (2)
- for that, find optimistic semantic minimization for $\neg R \wedge \neg(\neg P \vee AG(\neg R))$ and place it in (2):

$$\begin{aligned} \neg R \wedge \neg(\neg P \vee AG(\neg R)) &= \neg R \wedge P \wedge (\neg R \vee EX(EFR)) \\ &= \neg R \wedge P \wedge EX(EFR) \end{aligned}$$

- $\neg R \wedge P \wedge EX(EFR)$ is optimistically self-minimizing by our grammar

Example continued

- ... $\neg R \wedge P \wedge \text{EX}(\text{EFR})$ is optimistically self-minimizing by our grammar ...
- our grammar clause for EU and (Principle) then gives that

$$E[\neg R U \neg R \wedge \neg(\neg P \vee \text{AG}(\neg R))]^o = E[\neg R U \neg R \wedge P \wedge \text{EX}(\text{EFR})]$$

is optimistically self-minimizing

- folding the definition of AW, gives optimistically self-minimizing

$$\neg A[\neg P \vee \text{AX}(\text{AG}(\neg R))\text{WR}] \quad (3)$$

- finally, negate (3) to get desired pessimistic minimization:

$$A[\neg P \vee \text{AG}(\neg R)\text{WR}]^p = A[\neg P \vee \text{AX}(\text{AG}(\neg R))\text{WR}]$$

- this minimization forbids AG to refer to the present state, ensuring pessimistic self-minimization

Summary

- We showed that all patterns at

`patterns.projects.cis.ksu.edu`

are either pessimistically semantically self-minimizing, or have a pessimistic minimization with linear blowup only.

- The paper lists all this information in tabular form.
- These results assume that parameters of patterns are atomic, typical situation in practice. Our results remain to hold as long as parameters can be generated by our grammars.

Related work (discovered after our publication)

- Marsha Chechik & Arie Gurfinkel, How Thorough is Thorough Enough, CHARME 2005:
 - Given M and ϕ in universal fragment of CTL, one can construct M_ϕ , linear in M and exponential in the number of mixed-polarity atoms in ϕ such that $M \models^{th} \phi$ iff $M_\phi \models \phi$.

Related as our patterns are in that fragment. Our approach modifies formula once, works then for all models. Their approach modifies each given model and won't allow for mixed path quantifiers.

Acknowledgments

- Anonymous referees, for useful comments on the presentation of this paper
- UK Engineering and Physical Sciences Research Council for having funded this research under grant EP/D50595X/1